REMARKS

Claims 16, 17, 19, 21, 22, 26 are cancelled, claims 28 and 29 are amended, and claims 36-43 are added. The title is also amended to "DIGITAL RIGHTS SOURCE FOR XML KEY".

Rejection under 35 U.S.C. 103

On page 3 of the February 14, 2006 final Office Action, claims 16, 17, 19, 21, 22, 26 and 28-35 were rejected as unpatentable under 35 U.S.C. 103(a) over Pavlik (US Patent No. 6,807,633) further in view of Ginter et al. (US Patent Application Publication No. 2002/0112171), Carter et al. (US Patent Application Publication No. 2001/0021252) and Cato et al. (US Patent Application Publication No. 2003/0120928).
None of Pavlik, Ginter et al., Carter et al. or Cato et al. disclose or suggest that "the assembler comprises an XML encoder" operatively coupled "to add XML tags surrounding the permission information and surrounding the calculated digital signature when assembling the at least one digital rights key" as recited in independent claim 28 and associated dependent claims 29-35.

The first reference, Pavlik (US Patent No. 6,807,633), at col. 5, lines 32-53 renders a sample electronic document template 200 of the bank check illustrated in FIG. 2. Such would not have lead one to "add XML tags surrounding the permission information and surrounding the calculated digital signature" when assembling the key as recited in claims 28-35.

Neither of second and third references, Ginter et al. (US Patent Application Publication No. 2002/0112171) and Carter et al. (US Patent Application Publication No. 2001/0021252), refer to XML.

The fourth reference, Cato et al. (US Patent Application Publication No. 2003/0120928), discloses XML. However, the XML disclosed by Cato et al. (see for example the abstract) is applied prior to encryption and the XML is then encrypted. No key is disclosed and the XML is not applied to the key after its generation. Furthermore, Cato et al. are concerned with encryption, not authentication. In claims 28-35, the XML tag is added “surrounding the calculated digital signature” subsequent to calculation of the signature by the digital signature calculation block. The claims of the present inventions allow XML tags (e.g., the bracketed “< … >” tags illustrated in FIG. 7 of the instant disclosure) to wrap around the signature (e.g., “f52be709947cdd44cd72baf6773ebb95” in FIG. 7) and around the permission information. Wrapping XML tags around a previously calculated signature allows various decoders to interpret the signature and permission information between the XML tags without regard for their format or any future encoding incompatibility.

As for dependent claim 29, none of Pavlik, Ginter et al., Carter et al. or Cato et al. discloses or suggests “a selector for selecting a security parameter index among a plurality of security parameter indexes” and calculating the digital signature using “a security algorithm chosen based on the selected security parameter index” recited in claim 29. Such would not have rendered obvious using XML tags to surround a signature generated by a security algorithm chosen based on the selected security parameter index.

As for dependent claims 30 and 31 and 33, none of Pavlik, Ginter et al., Carter et al. or Cato et al. discloses or suggests an assembler for assembly of a digital rights key having both a digital signature and permission information, wherein the permission information comprises a destination identifier or a type designation recited in dependent claims 30 and 31. Dependent claim 32 further recites that the permission information used by the digital signature calculation block and the assembler further comprise a feature ID and a number of feature units. The present invention makes and sends a key where permission information is not only sent alongside the signature, but that same permission information is sent together with the signature to the recipient. This permission information is even sent in clear text as recited in claim 33. The recipient then can decode the key in the same was as it was encoded – by using the permission information received and the known security parameter index to decode the digital signature. Pavlik, Ginter et al., Carter et al. or Cato et al. do not disclose a destination identifier and a type designation used for both encryption of the signature and assembly of the key along with permission information in clear text or a feature ID and a number of feature units as recited in claims 30, 31, 32 or 33.

Accordingly, reconsideration and withdrawal of the rejection of claims 28-35 under 35 U.S.C. § 103(a) as unpatentable over Pavlik further in view of Ginter et al., Carter et al. and Cato et al. is respectively requested.

Conclusion

For the foregoing reasons, pending claims 28-35 and new claims 36-43 should be in condition for allowance. The Examiner is encourged to contact the Applicants' Representative at the below-listed telephone number if there are any questions or concerns that may expedite prosecution.

Respectfully submitted,

Marko W. Pfaff et al.

By their Representatives,

By ______________________________
Daniel W. Juffernbruch
Reg. No. 33,122
847-458-6313

Patents and Licensing LLC
28 Barrington Bourne
Barrington, IL 60010-9605
tel: 847-458-6313
fax: 815-301-8408
Dan@patentsandlicensing.com